



R&DTM

November 2004

2005 Lab Design Handbook


From the Editors of
R&D Magazine and
Laboratory Design newsletter

How to build a lab from start to finish, including information on:

- The Big Picture
- Costs and Budgets
- Mechanical Systems
- Utility and Security Infrastructure
- Design Trends
- Sustainability
- Specialty Labs
- Renovation, Leasing, and Construction
- On-line Information Resources

PLUS: Exclusive directory of architecture, engineering, construction, and consulting firms.

www.labdesignnews.com
www.rdmag.com

 Reed Business
Information.

Supplement to R&D Magazine

RISK ANALYSIS FOR LABORATORY SECURITY

Designing infrastructure that suits the threat potential and consequences

By Natalie Barnett

Now more than ever, people are aware of biological weapons and the threat of bioterrorism. Bioscience research facilities have come under scrutiny as a potential source of viable and virulent pathogens that could be used as a weapon. The federal government enacted legislation in 2001 and 2002 in an effort to reduce the risk that biological materials could be indiscriminately accessed and removed from these facilities. (For legislative details, see box on page 42.)

These new legal requirements, along with pressure to address public concerns, have led some institutions to implement security systems that are often perceived by the scientific community as onerous, ineffective, and expensive. Bioscience facilities generally represent the cutting edge in terms of lab building security, and can provide important lessons for other types of buildings. Many of these security systems are dominated by significant levels of physical security and are designed to protect against an overwhelming outside threat.

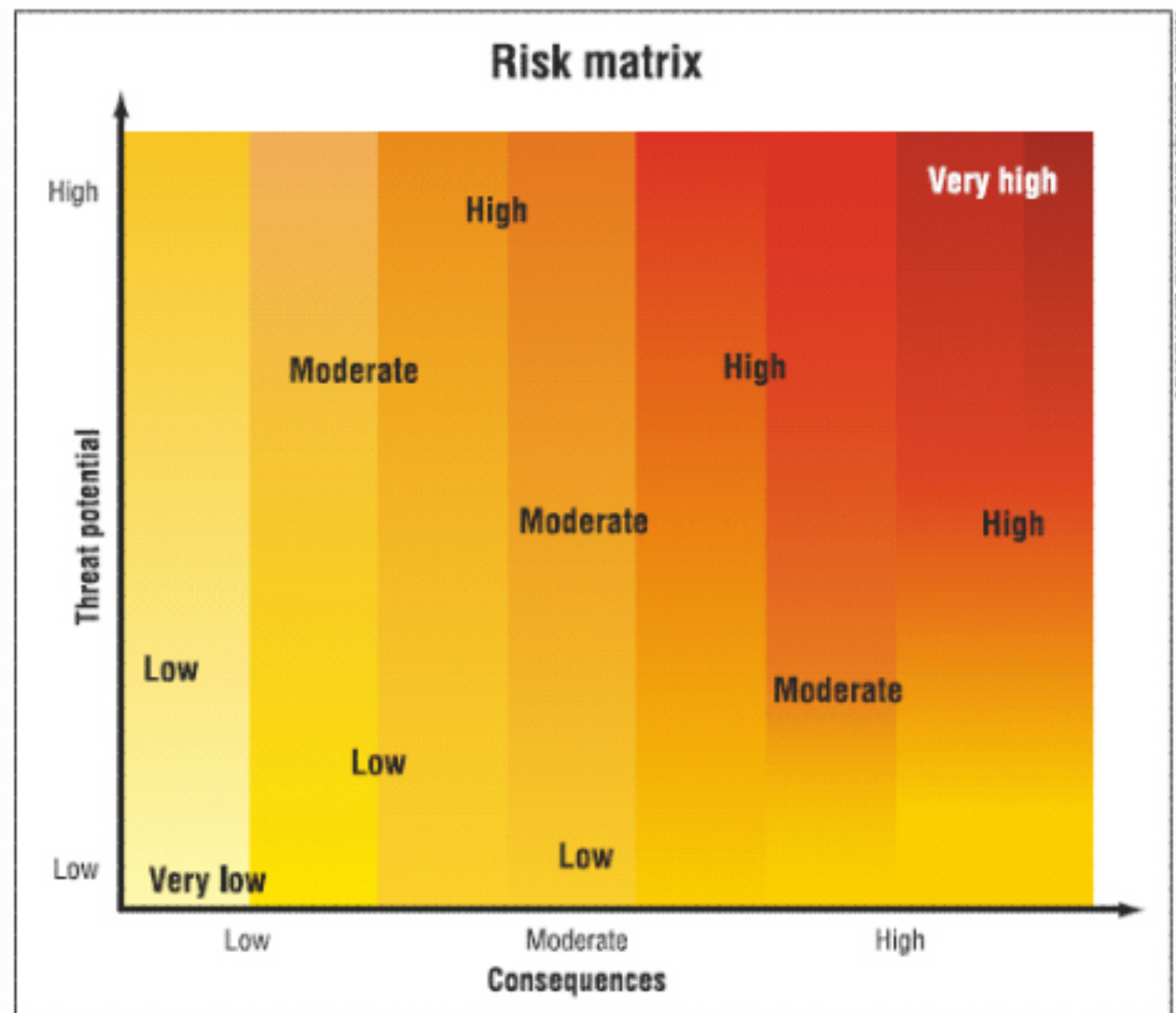
Physical security is a necessary component of laboratory design, and therefore is highlighted in this article, but it is only one, relatively small, element of a complex solution. Policies and procedures regarding access to, and control of, biological materials play a much more significant role in protecting lab contents from theft and sabotage than physical security measures. To design a suitable and cost-effective security system, it is critical to understand the risks associated with biological research facilities and to address them in a manner that incorporates the unique properties of biological assets and the adversaries who threaten them.

Assessing and managing risk

The U.S. Government Accountability Office endorses a risk management approach to security. The method establishes which assets should be protected against which threats, and ensures that the amount of protection provided to a specific asset, and the cost for that protection, is proportional to the risk of the theft or destruction¹. Risk management begins with a risk assessment. Key steps are:

- **Characterize the facility.** Understand the mission, operations, processes, policies, and procedures. Examine blueprints locating the assets, and methods and pathways of access (doors, windows, etc.).

- **Define the assets.** Assets at a bioscience facility may include biological materials, security-related or proprietary information, people, power systems, lab equipment, and buildings.
- **Evaluate the consequences** of an asset being used to achieve an undesirable event (e.g. theft and use, or sabotage). The consequences associated with biological terrorism are often associated with the infectious disease characteristics of the agent used, which may include infectivity,



Natalie Barnett/US and National Laboratories

pathogenicity, lethality, and transmissibility.

- **Identify the adversaries** who might try to perpetrate an undesirable event, and evaluate the potential threat they pose. Define their characteristics, motivations, and capabilities. Adversaries may include insiders with full access to the asset (staff scientists and lab technicians); restricted-access insiders (visiting scientists, staff maintenance personnel); outsiders with limited access (delivery personnel, repair personnel, non-staff maintenance personnel); and outsiders with no normal access (political extremists, psychotic individuals).
- **Evaluate the level of risk the adversary would incur** in executing the undesired event and the attractiveness of the asset. The attractiveness of a particular biological agent as a weapon may depend not only on its public health conse-

Fig. 1. A risk matrix is a graphic way of weighing the threat potential against the possible consequences.

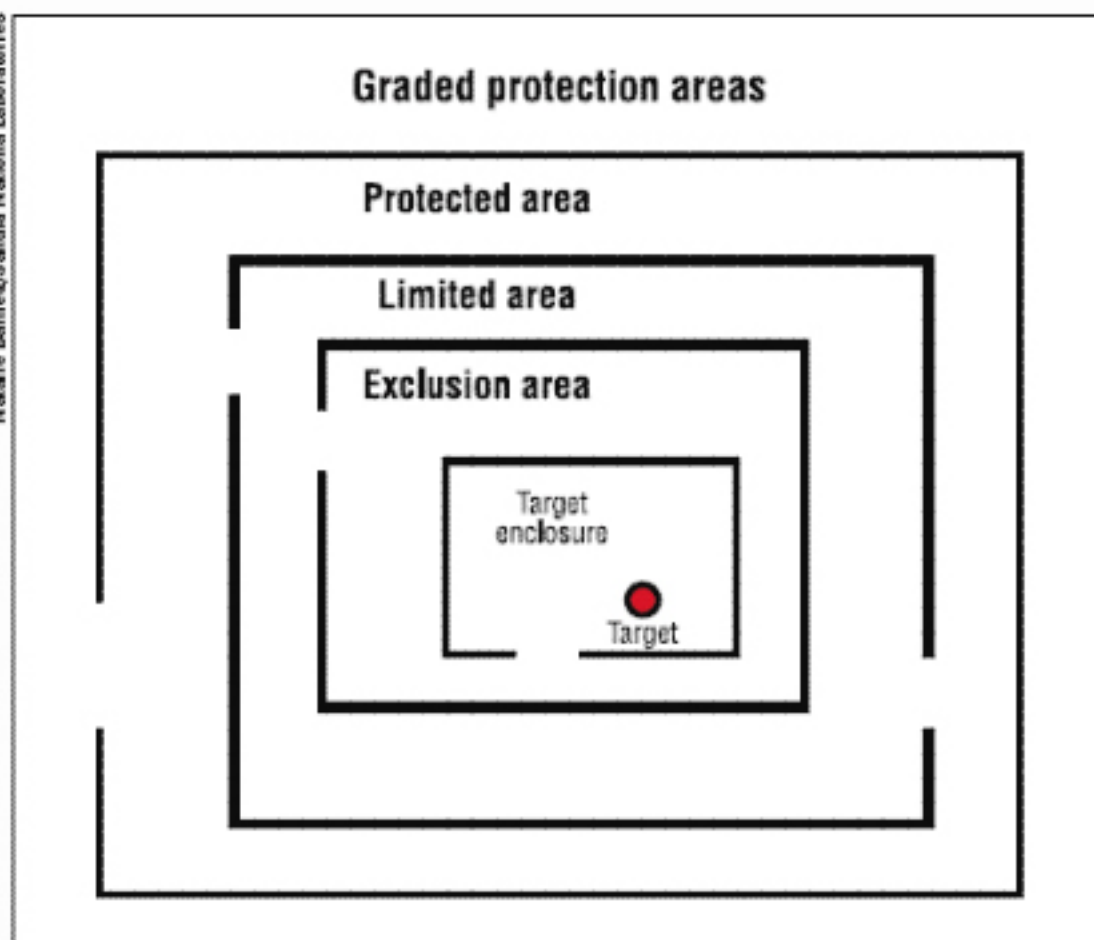


Fig. 2. A site can achieve graded protection by increasing the level of security as the value of the asset to an adversary increases, and as the location of the asset is approached

quences but also on its availability, ease of amplification, ease of processing, environmental hardness, available countermeasures, and ability to be camouflaged as an endemic or common disease.

- *Evaluate the risk.* Risk is a function of the potential threat posed by the adversary and the consequences of a successfully executed attack. The risk matrix on page 41 provides a graphic way of weighing the threat potential against the possible consequences.
- *Determine which risks to protect against.* The risk assessment should help management understand what needs to be protected, who it should be protected from, and the consequences of a protection failure. Failing to adequately protect an asset could allow an adversary to successfully execute a malevolent act, while overprotecting a nonessential asset wastes limited resources.
- *Conduct a vulnerability analysis.* Are there gaps in the existing security that would allow the unacceptable risks to materialize?

Insiders vs. outsiders

Insiders tend to pose a higher threat potential than other types of adversaries. Insiders have a high level of access to the facility and its assets, as well as operational knowledge, technical ability, and the ability to illicitly remove materials from a lab without being seen or otherwise observed. The threat outsiders pose to biological agents is limited by the facts that most pathogens are also available in nature, most outsiders have limited operational knowledge of the facility, and authorities can deploy countermeasures to mitigate an attack if a theft is discovered.

The likelihood of deterring or detecting a covert attack by an outsider, or theft by an insider, is considerably higher when some form of physical security is in place. Limiting access to important assets, and detecting unauthorized access, are effective strategies for minimizing the opportunities for covert attack by an adversary who does not have authorized access.

Overt theft of a biological asset by an outside adversary is a low risk for most biological facilities. Most facilities do not have biological materials that are unique or valuable enough as a weapon to warrant the risk an adversary would incur by stealing and trying to use the materials. After comparing the low risk

New legislation affecting the biological sciences

USA Patriot Act

- Prohibits “restricted persons” from shipping, receiving, transporting, or possessing certain pathogens.

Bioterrorism Preparedness Act

- Requires the Department of Health and Human Services (HHS) to establish and maintain a list of biological agents and toxins with the potential to pose a severe threat to public health and safety, including those that are zoonotic (communicable from animals to humans under normal conditions).
- Requires the U.S. Department of Agriculture (USDA) to establish and maintain a list of particularly dangerous plant, animal, and zoonotic pathogens and toxins.
- Mandates that laboratories that possess any of these biological agents or toxins improve security to preclude access to these materials by “restricted persons” or others who may have malicious intent.

Codes of Federal Regulation (CFRs)

The HHS and USDA lists mandated by the Bioterrorism Preparedness Act are codified in three Codes of Federal Regulation: 42 CFR Part 73 (human and zoonotic); 9 CFR Part 121 (animal and zoonotic); and 7 CFR Part 331 (plant). There are specific physical security elements in the CFRs that include:

- “Establishing procedures for securing the area (e.g., card access system, key pads, locks), including protocols for changing access numbers or locks following staff changes.”
- “Providing for the control of access to containers where select agents and toxins are stored ... when they are not in the direct view of approved staff, and by using other monitoring measures as needed, such as video surveillance.”

against the high cost of protecting against such an attack, many facilities may decide to accept that risk. Others may decide that the risk is high enough to warrant addressing it through incident response planning. Still others may decide to protect themselves against such an attack, either because the assets they hold warrant such action or because their management believes, for any number of reasons, that the facility must implement an expensive, risk-averse, security posture.

Biosecurity protection principles to address the inside adversary may include:

- Scientific program oversight.
- Personnel security program.
- Information system security.
- Material control and accountability.
- Chain-of-custody procedures for transfer of dangerous pathogens and toxins.
- Access controls.
- Alarm assessment and response capability.

Biosecurity protection principles to address the outside adversary may include:

- Visitor screening and escort procedures.
- Information system security.
- Material control and accountability.
- Intrusion detection and access controls.
- Alarm assessment and response capability.

Creating graded areas

Incorporating these principles in a facility's biosecurity design is particularly effective when a graded approach is taken. A site can achieve graded protection by increasing the level of security as the value of the asset to an adversary increases, and as the location of the asset is approached. Zones of security, in order of increasing access-control and protection, include the "protected area," the "limited area," and the "exclusion area," all surrounding the target enclosure (Fig. 2).

- *Protected areas* are areas containing low-security assets, including the building grounds and public-access areas. Primary protection methods include fences and signage that mark the property boundary and discourage people from strolling onto the property.
- *Limited areas* contain moderate security assets. Examples include labs containing moderate risk² pathogens, administrative offices containing sensitive information, and hallways surrounding exclusion areas. Protection

methods include structural hardening (minimal penetrations such as doors, windows, ducts, vents, etc.; balanced strength between doors, windows, and walls). Access controls for limited areas usually involve a unique credential, such as an electronic key card or

a controlled mechanical key.

- *Exclusion areas* are those containing high-security assets, such as labs containing high-risk pathogens; computer network hubs; and security control rooms. In addition to the kind of structural hardening used for the limited

Who chooses YOUR Lab Monitoring System?



Don't settle for a solution without knowing your options in advance. Make sure the end product meets YOUR needs and expectations!

With your input,
REES SCIENTIFIC
will help you make
product choices
that best suit ALL
of your **Facility
Monitoring**
requirements.



Rees Scientific. The difference is in the details.

**Environmental Monitoring
Access Control Systems**

**REES
SCIENTIFIC**
An ISO 9001 Company

If you're planning a new facility or renovating an existing facility, please call us to arrange a brief demo!

Use InfoLINK 4L3110 or Call 800-843-1014
1007 Whitehead Rd. Ext., Trenton, NJ 08638
800.327.3141 Fax: 609.530.1854
sales@reesscientific.com/www.reesscientific.com

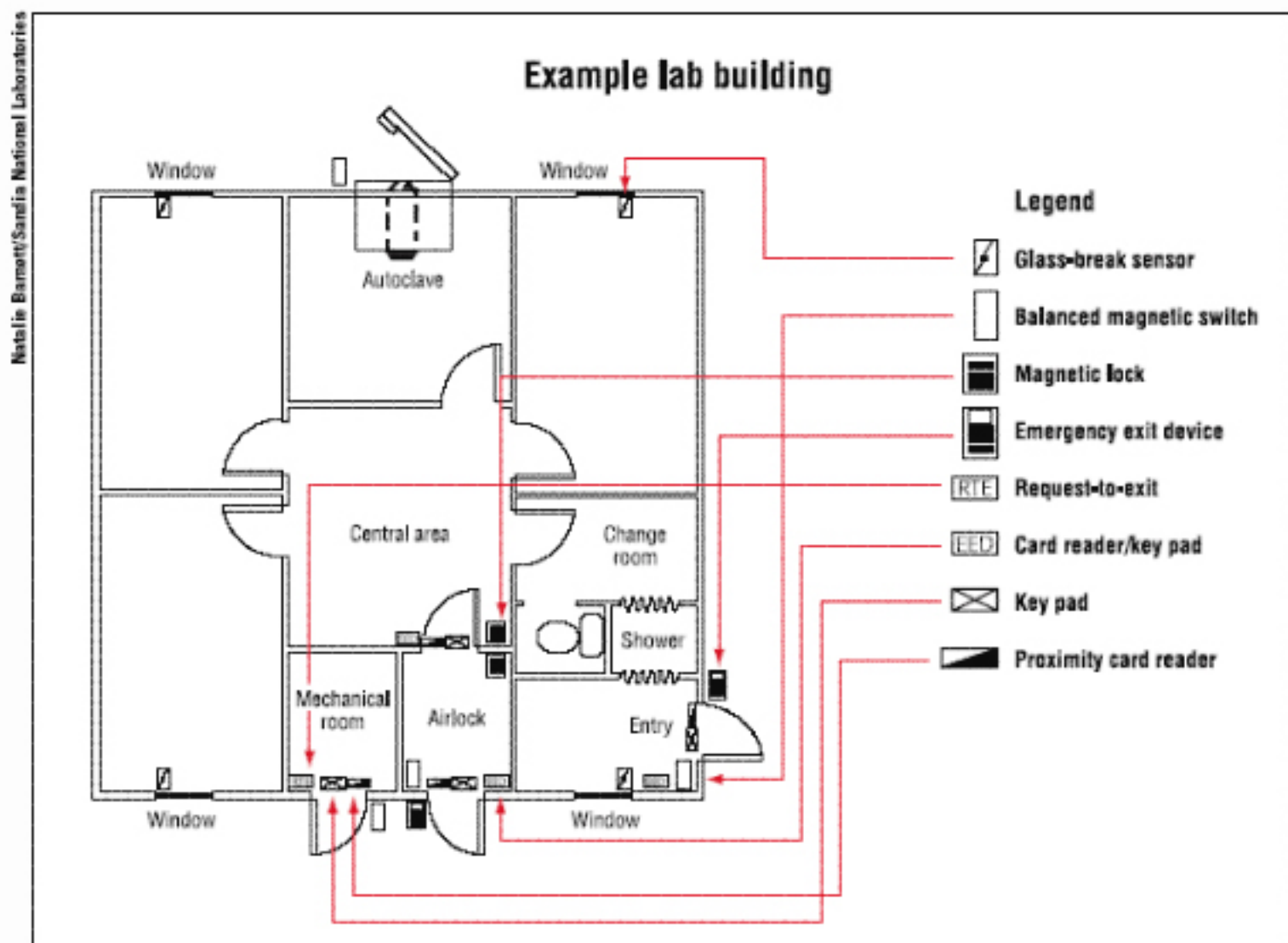


Fig. 3. A sample lab layout based on graded security areas.

areas (above), exclusion areas typically involve more stringent access controls, which will combine a unique credential plus some type of unique knowledge. The unique credential could be an electronic key card/keypad or biometric device, or a controlled mechanical key plus an individual to verify the entrant's identity.

Fig. 3 shows a sample layout for a lab with security based on graded areas. In addition to the considerations noted above, the design should create "nor-

mal" paths for employees and visitors that enforce applicable checkpoints without providing alternate, unsecured, routes. Emergency egress paths should not channel individuals into areas where they would not normally have access.

Legal compliance and good stewardship both require labs to protect dangerous pathogens and toxins from malicious use. Well-founded biosecurity starts with a bioscience-specific risk assessment and is followed by a biosecurity design that is based on graded protection principles, policies, and procedures. The biosecurity design process should incorporate input from experts in biological weapons, security systems, the biological sciences, architecture, and engineering for the results to be the most effective and the least intrusive. The design and implementation of the biosecurity system will determine whether it supports the objectives of security and science, or is an impediment to either or both.

References

1. U.S. GAO. "Homeland Security: A Risk Management Approach Can Guide Preparedness Efforts," GAO-02-208T (Washington, DC: October 2001). Also see U.S. GAO, "Combating Bioterrorism: Actions Needed to Improve Security at Plum Island Animal Disease Center," GAO-03-847, (Washington, DC: September 2003).
2. See "A Conceptual Framework for Biosecurity Levels," by Jennifer Gaudioso and Reynolds M. Salerno, February 2004, SAND 2004-0759C, for a discussion of risk levels for pathogens and toxins. <http://www.biosecurity.sandia.gov/documents/conceptual-framework-biosecurity-levels.pdf>

Natalie Barnett is a biosecurity systems analyst at Sandia National Laboratories, Albuquerque, N.M., She is currently part of a Sandia team that is working with federal agencies in the U.S. to develop biosecurity plans to address protecting dangerous pathogens and toxins from theft and illicit diversion. Her work includes performing risk, threat and vulnerability analyses of microbiological research facilities; designing biosecurity systems; overseeing implementation of these systems; and writing and implementing biosecurity policies and procedures.